order of element $G = \langle Z_7^*, x \rangle$

$i = 1, 2, 3 \ldots$ $a^i = x \pmod{n}$

i = order of element

~~Re~~ Primitive Root

Group $G = \langle Z_p^*, x \rangle$

order of Group $\phi(p)$

where $\phi(1) = 0$

$\phi(p) = p-1$, if p is prime

$\phi(m \times n) = \phi(m) * \phi(n)$

m & n are relatively prime

$\phi(p^e) = p^e - p^{e-1}$

if p is prime

$\Rightarrow$ In the group, $G = \langle Z_n^*, x \rangle$

when the order of element is the same as $\phi(n)$,

that element is called the primitive root of the group.

Scanned by CamScanner

$x \equiv y \pmod{n}$ $Z_p^* \rightarrow$ set of all relative primes of p

* Elgamal Cryptosystem

Key Generation

① Select a large prime p

② select d to be a member of the group $G = \langle Z_p^*, \times \rangle$

such that $1 \leq d \leq p-2$

select e_1 to be primitive root in the group $G = \langle Z_p^*, \times \rangle$ $\longrightarrow$ $\phi(p)$

$a^i = x \pmod{n}$

$e_2 = e_1^d \bmod p$

public key $= \{e_1, e_2, p\}$ $\left[\underset{p}{q}, \underset{e_1}{\alpha}, \underset{e_2}{Y_A}\right]$

private key $= d$.

Encryption

① select integer r in the group

$G = \langle Z_p^*, X \rangle$

$C1 = e_1^r \bmod p$

$C2 = (P * e_2^r) \bmod p$

Decryption

$P = [C_2 (C_1^d)^{-1}] \bmod p$

Ex:

$p = 11$, $e_1 = 2$

2 is primitive root in Z_{11}^*

$d = 3$,

$e_2 = e_1^d = 8$

public key = (2, 8, 11)

private key = 3

Plaintext P = 7

r = 4 $c_1 = ?$ $c_2 = ?$

Ans

$c_1 = e_1^r \bmod 11 = 16 \bmod 11 = 5$

$c_2 = (P * e_2^r) \bmod 11$

$= (7 * 4096) \bmod 11$

$= 6$

now

$P = C_2 (C_1^d)^{-1} \bmod P$

$= 6 (5^3)^{-1} \bmod 11$

$= 6 * 3 \bmod 11$

$\boxed{(125 * 3) \bmod 11 = 1}$ ← multiplicative inverse modulo

$= 7 \mod 11$

$P = 7$ ← plaintext

* known-plaintext Attack

Same random no. r to encrypt two plaintext P and P'

P' can be discovered by using P'

$$C_2 = P \times (e_2^r) \bmod p$$

$$C_2' = P' \times e_2^r \bmod p$$

$$\Rightarrow (e_2^r) = C_2 \times P^{-1} \bmod p$$

$$P' = C_2' \times (e_2^r)^{-1} \bmod p$$